

# Procedure Manual



<b>Title: Criminal Justice Information Handling and Storage (Employee Handling of Records for Students and Applicants for Admission)</b>	<b>Number:</b> A6Hx2-3.55B
<b>Policy Number:</b> 6Hx2-3.55	<b>Page:</b> Page 1 of 8

## Personally Identifiable Information (PII)

Personally-Identifiable Information (PII) is any information pertaining to an individual that can be used to distinguish or trace a person's identity. PII is defined as any one or more of types of information including, but not limited to:



1. Social security number
2. Username and password
3. Passport number
4. Credit card number
5. Clearances
6. Banking information
7. Biometrics
8. Data and place of birth
9. Mother's maiden name
10. Criminal, medical and financial records
11. Educational transcripts
12. Photos and video including any of the above

All electronic files that contain PII will reside within the College in a physically secure location. All physical files that contain PII will reside within a locked file cabinet or room when not being actively viewed or modified.

PII is not to be downloaded to workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media) or to systems outside the protection of the College. PII will also not be sent through any form of insecure electronic communication as significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII, the physical or electronic file should be shredded or securely deleted. All disposals of PII will be done by authorized College employees.

All PII will be collected only when there is a legal authority and it is necessary to conduct college duties. Access to PII is only conducted when the information is needed to conduct College official duties and should only be utilized for official purposes.

College employees will not create duplicate copies of documents that contain PII and will destroy the documents when no longer needed. When PII is extracted from a document, College employees may only target the PII that is required for the task. PII that is extracted shall not be retained beyond the records retention rules for the data and the system it was accessed from. PII shall not be stored or transmitted via personally owned devices. PII may not be taken home by any College employee.

<b>Recommending Officer's Signature:</b> 	<b>Date:</b> 5/03/2022	<b>President's Signature:</b> 	<b>Date:</b> 5/03/2022
---	---------------------------	--	---------------------------

# Procedure Manual



<b>Title: Criminal Justice Information Handling and Storage (Employee Handling of Records for Students and Applicants for Admission)</b>	<b>Number:</b> A6Hx2-3.55B
<b>Policy Number:</b> 6Hx2-3.55	<b>Page:</b> Page 2 of 8

## Information Handling

The employees assigned to review background checks have workstations that are encrypted with FIPS 140-2 certified encryption. Physical information, such as reports that contain criminal justice information, is not printed, except for instances in which the file must be shared with the student and is documented. If as part of this exchange, a file is lost, stolen, or missing, then the incident must be reported to the College Local Agency Security Officer (LASO). The following action must then be taken to mitigate the security incident:

- locate the missing file,
- determine how and who caused the incident,
- notify the FDLE Information Security Officer by emailing [fdlecjisiso@flejn.net](mailto:fdlecjisiso@flejn.net).



## Information Exchange

Criminal Justice Information is the term used to refer to all of the FBI CJI provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJI architecture:

1. **Biometric Data**—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. It is used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. **Identity History Data**—textual data that corresponds with an individual’s biometric data, providing a history of criminal and/or civil events for the identified individual.
3. **Biographic Data**—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. **Property Data**—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. **Case/Incident History**—information about the history of criminal incidents.

## Incident Response

All users are responsible for reporting known or suspected information or information technology security incidents. All incidents must be reported immediately to the College Local Agency Security Officer (LASO). The LASO will inform a member of IT and document the incident. If a suspected incident occurs on the FDLE CJIS workstation, the user shall not turn off the device. The user will leave the device on and report the incident. The College will employ Microsoft System Center Endpoint Protection on the desktop and will ensure that the antivirus software is up-to-date. Incident response will be managed based on the level of severity of the incident. The level is a measure of its impact or threat on the operation or integrity of the College and its information. High Level (potential to impact the desktop or criminal justice information) Medium Level (potential to impact

<b>Recommending Officer’s Signature:</b> 	<b>Date:</b> 5/03/2022	<b>President’s Signature:</b> 	<b>Date:</b> 5/03/2022
---	---------------------------	--	---------------------------

# Procedure Manual



<b>Title: Criminal Justice Information Handling and Storage (Employee Handling of Records for Students and Applicants for Admission)</b>	<b>Number:</b> A6Hx2-3.55B
<b>Policy Number:</b> 6Hx2-3.55	<b>Page:</b> Page 3 of 8

a non-critical system) Low Level (has little or no risk of infecting a criminal justice system). If the level is moved to High, the LASO will notify FDLE immediately. All security incidents will be documented on a security incident reporting form, kept by the LASO and retained for no less than a three year period.

## Account Management

The College's LASO is the point of contact for all accounts. The LASO shall manage information system accounts to include establishing, activating, modifying, reviewing, disabling, and removing user accounts on all Criminal Justice Information Systems.



## Account Creation

1. The LASO will create and establish a Windows Domain account for the applicant. Each account is uniquely identified by the user's college email address which is derived from the user's first letter of the first name followed by seven digits of the last name. All accounts are created to ensure a unique username for every individual.
2. The Domain account will be assigned a temporary password and will be set up to require the user to create a new password upon activating the first session. The password for the account must adhere to the College's password requirements outlined in the Authentication Strategy Policy.
3. The LASO will identify the level of authority for the user for each application.
  - Admin
  - User
  - Records
4. The LASO will provide the initial credentials and temporary password to the users' supervisor.
5. Mobile devices are not used for CJI access.
6. The LASO will meet with the new user upon starting to ensure proper access to each information system is granted.

## Account Modification

In the event of promotion, demotion, suspension, leave or voluntary or involuntary termination, the supervisor will immediately notify the LASO of the change of status to ensure appropriate access changes are made to systems and applications.

1. Promotion/Demotion  
Supervisor will notify LASO of the change of status and change of authority level.
  - The LASO will update all systems and applications as necessary to evolve with the current status of employment and will document these changes in the active directory.
2. Suspension/Leave  
Supervisor will notify LASO of the temporary change to the user's account.
  - The LASO will temporarily deactivate the account on each system and application.
  - Upon reinstatement, the supervisor will notify the LASO.
  - The LASO will reactivate the user accounts on all systems and applications.

<b>Recommending Officer's Signature:</b> 	<b>Date:</b> 5/03/2022	<b>President's Signature:</b> 	<b>Date:</b> 5/03/2022
---	---------------------------	--	---------------------------

# Procedure Manual



<b>Title: Criminal Justice Information Handling and Storage (Employee Handling of Records for Students and Applicants for Admission)</b>	<b>Number:</b> A6Hx2-3.55B
<b>Policy Number:</b> 6Hx2-3.55	<b>Page:</b> Page 4 of 8

- The user will verify that the accounts are active.

## Account Termination

- Upon termination from the College, whether voluntary or involuntary, the supervisor will inform the LASO of the employment change.
- The LASO will disable all accounts on all information systems and applications.
- The LASO will place the user in the Disabled User Organizational Unit within Active Directory, remove all access of controls from the user, disable the College's e-mail account, and remove remote access ability and all permissions.

## Account Validation

- The LASO will validate the College's User Accounts and Access Privilege Levels annually.
- The LASO will document the date and time of the validation on the College's Validation Form.
- The LASO will verify that all active accounts are current and up-to-date.
- Any changes made by the LASO involving an account will be documented.

## Reviewing Account

The user accounts will be reviewed weekly using the security logs.

## Access Control

Access to College information system(s) are based on a user's right to know, authority, and user group. The College does not allow multiple concurrent sessions on FDLE CJIS workstations.

## Validation Process for Annual Review



- At the beginning of every fiscal year, the LASO will review all staff access to CJI data
- Log into CJIS Online and verify employees with access
- Verify with supervisors the status of employees with access to CJI data
- Inactivate those employees who no longer require access to CJI data
- Add employees who may need CJI access based on changes in employment
- Ensure that new employees complete CJI training and assessment
- Maintain a log file that provides the results of this process
- Coordinate with supervisors of employees with CJI access to inform the LASO of terminations, promotions etc.

## Remote Access

The College does not allow remote access to the FDLE CJIS workstation.

## Personally-Owned Information Systems Access

The College does not allow personally owned devices to access, store or transmit criminal justice information.

<b>Recommending Officer's Signature:</b> 	<b>Date:</b> 5/03/2022	<b>President's Signature:</b> 	<b>Date:</b> 5/03/2022
---	---------------------------	--	---------------------------

# Procedure Manual



<b>Title: Criminal Justice Information Handling and Storage (Employee Handling of Records for Students and Applicants for Admission)</b>	<b>Number:</b> A6Hx2-3.55B
<b>Policy Number:</b> 6Hx2-3.55	<b>Page:</b> Page 5 of 8

## Authentication Strategy

This Password Policy applies to all information systems and applications that contain criminal justice information or services. This includes, but is not limited to:

- FDLE CJIS workstation
- Mainframes, servers and other devices that provide centralized computing capabilities
- SAN, NAS and other devices that provide centralized storage capabilities
- College issued desktops, laptops, or any other device that provides distributed computing capabilities
- Routers, switches and other devices that provide network capabilities
- Firewalls and other devices that provide dedicated security capabilities
- Windows Domain Accounts, college e-mail accounts, as well as any other criminal justice information system or service

Each account is set up with a temporary password. When the user initiates a first-time log-on, the temporary password will be entered, and the user will be prompted to create a new password. The College dictates that each password and User-ID be unique and not be shared with any other individual. Users are forbidden to share or record their unique password. All passwords must be memorized.



## Password Requirements

The College utilizes individual passwords for gaining access to criminal justice information and systems. As such, all passwords must follow the requirements outlined below:

- College user passwords must contain at least 8 characters
- The user may not use a proper name or a dictionary word as a password
- The user cannot use their user-id as the password
- The password is set to expire every 60 days
- The user cannot reuse the previous 10 passwords
- The password cannot be transmitted in the clear outside the secure location
- The password will not be displayed when entered

## Authenticator Management

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, one-time passwords (OTP) and personal identification numbers (PIN). Authenticators will be assigned to personnel during training or upon reassignment. A temporary standard authenticator is given to the user via the LASO during the first active session the user has. The user then creates a new password outlined in the authentication strategy policy. Any compromised authenticator should be reported to the **IT department** immediately. An Authenticator shall be deactivated immediately if personnel is terminated, retired, or has been reassigned. An Authenticator can be deactivated by contacting the Helpdesk which will initiate a ticket and the user will de-activated.

<b>Recommending Officer's Signature:</b> 	<b>Date:</b> 5/03/2022	<b>President's Signature:</b> 	<b>Date:</b> 5/03/2022
---	---------------------------	--	---------------------------

# Procedure Manual



<b>Title: Criminal Justice Information Handling and Storage (Employee Handling of Records for Students and Applicants for Admission)</b>	<b>Number:</b> A6Hx2-3.55B
<b>Policy Number:</b> 6Hx2-3.55	<b>Page:</b> Page 6 of 8

## Media Protection Management

Media in all forms (electronic and physical) shall be protected at all times. Media is restricted to authorized individuals. Only those users of the Agency who have appropriate security awareness training will be allowed to handle criminal justice information in any form.

Electronic media (i.e. hard drives, disks, flash drives, servers, etc.) shall be behind locked doors at all times with access granted only to authorized personnel. Any computer that accesses criminal justice information within the facility will have a screen cover to ensure that information is not viewable by any unauthorized individual. CJI shall be destroyed when not in use by procedures notated in the disposal of electronic media sanitization and disposal policy.

Physical media (i.e. physical documents) shall only be stored until admission decisions are finalized. CJI stored will be placed in a locked filing cabinet behind locked doors. Only authorized personnel will be granted access. CJI shall be destroyed when not in use by procedures notated in the disposal of physical media policy.

Any media that is transported outside the physically secure location will be in a sealed envelope to ensure security is maintained. All activities associated with transport of media must be completed by authorized personnel only.

When the media is released to another user, the user will document the transaction in a secondary dissemination log for validation purposes. At no time will the physical media be released to an unauthorized person or left without proper documentation.

## Electronic Media Sanitization and Disposal

All electronic media must be properly sanitized before being transferred from the custody of the College. The proper method of sanitization depends on the type of media and the intended disposition of the media.

Hard Drives: The College will overwrite the hard drive utilizing a three pass wipe. This will ensure that the data on the drive is overwritten with patterns of binary ones and zeros. The sanitization of the hard drive is not complete until the third wipe passes, and a verification pass is complete. Destruction of the hard drive will incorporate drilling into the drive.



## Disposal of Physical Media

When no longer needed, physical media such as hard copy print-outs shall be disposed of by the following method:

- Shredded using a college owned cross-cut shredder. The shredding will be done by authorized college employees. All forms of destruction of physical media will be witnessed or carried out by authorized agency personnel.

## Physical Protection

Physically Secure Location:

<b>Recommending Officer's Signature:</b> 	<b>Date:</b> 5/03/2022	<b>President's Signature:</b> 	<b>Date:</b> 5/03/2022
---	---------------------------	--	---------------------------

## Procedure Manual



<b>Title: Criminal Justice Information Handling and Storage (Employee Handling of Records for Students and Applicants for Admission)</b>	<b>Number:</b> A6Hx2-3.55B
<b>Policy Number:</b> 6Hx2-3.55	<b>Page:</b> Page 7 of 8

The agency's hardware, software, and media containing confidential information will be protected through access control measures. Media will be restricted to only College authorized personnel.

Physical media will be stored behind locked doors in a locked filing cabinet. Only authorized personnel with a "need to know" or "right to know" based on job duties will have access.

### **Encryption**

The FDLE CJIS workstation drive has been encrypted using BitLocker and FIPS encryption has been enabled. PKI encryption is not utilized.



### **Voice over Internet Protocol**

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. There are no VoIP phones connected to the FDLE CJIS workstation.

The agency will ensure the following usage restrictions for College personnel:

- Do not divulge personal or criminal justice information to people you don't know.
- Be cognitive of discussing criminal justice information using your VOIP Phone on Speaker with unauthorized personnel in the room.
- Do not discuss CJI data with other staff utilizing on your VOIP phone.
- Do not install or connect devices to your VOIP Phone such as computers, Bluetooth, recording device, etc.
- VOIP phone should not be used for international use (outside the United States and its territories).
- Do not store or save criminal justice information on VOIP System.
- If power is lost to the VoIP adapter or if your internet connection is lost due to a power outage, you will be without phone service. Please ensure that your VOIP Phone is connected to the red or orange electrical outlet that provides generated power in case of power outage.
- Do not connect fax machine into VOIP System to fax criminal justice information.
- If your VOIP Phone System does not provide a dial tone or is not showing the correct time/date and extension, please alert Information Technology (IT) by email, cellular phone or walk-in visit to complete an incident and or work order. The IT department may determine if it is a malicious code (i.e., worms, viruses, trojans), denial-of-service (DoS), distributed DoS (DDoS), and (though non-malicious) flash crowds event.

<b>Recommending Officer's Signature:</b> 	<b>Date:</b> 5/03/2022	<b>President's Signature:</b> 	<b>Date:</b> 5/03/2022
---	---------------------------	--	---------------------------

# Procedure Manual



<b>Title: Criminal Justice Information Handling and Storage (Employee Handling of Records for Students and Applicants for Admission)</b>	<b>Number:</b> A6Hx2-3.55B
<b>Policy Number:</b> 6Hx2-3.55	<b>Page:</b> Page 8 of 8

## Patch Management

FDLE CJIS workstations owned by the college must have up-to-date operating system security patches installed in order to protect the device and network from known vulnerabilities.

IT will manage the patching needs for the FDLE CJIS workstations. IT will routinely assess the compliance of the patching policy and will provide guidance to all employees of any security and patch management issues. IT also approves monthly and emergency patch deployments if necessary.

## Security Alerts and Advisories

The IT Department will monitor and/or receive alerts and advisories from the locations listed below. If an alert is determined to be critical or pertinent to college infrastructure, the appropriate employees will be notified. All alerts and related actions will be recorded into an information log for college records.

The IT department has signed up for alerts and advisories from the following sites:

- [www.us-cert.gov/ncas/current-activity](http://www.us-cert.gov/ncas/current-activity)
- <https://tools.cisco.com/security/center/publication>
- <https://technet.microsoft.com/en-us/security>

1. IT will take appropriate action depending on the alert. This could include updating security settings and/or issuing information to all relevant college employees with directions to ensure proper handling of the issue.
2. IT will document the details of the alert. The log will remain with IT for a period of four years.
3. The College will receive information system security alerts and advisories
4. Once an alert has been received or detected and has been determined to be a credible threat, IT will notify the College LASO.
5. The College will receive information system security alerts and advisories
6. Once an alert has been received or detected and has been determined to be a credible threat, IT will notify the College LASO.

## Wireless Access Restrictions



Wireless technology is not utilized by the College to connect or transmit any of FDLE CJIS data.

## Review of Wi-Fi Logs

Wireless technology is not utilized by the College to connect or transmit any of FDLE CJIS data.

## Bluetooth

Bluetooth technology is not utilized by the College to connect or transmit any FDLE CJIS data.

<b>Recommending Officer's Signature:</b> 	<b>Date:</b> 5/03/2022	<b>President's Signature:</b> 	<b>Date:</b> 5/03/2022
---	---------------------------	--	---------------------------